

A case study of Gröbner bases and Hilbert series

Soutrik Roy Chowdhury *

Abstract

In this expository writing I will give an introduction to Gröbner bases and how to use it to compute Hilbert series from chains.

Key words: Diamond lemma, normal monomials, Hilbert series.

Contents

1	Introduction	2
2	Background for Gröbner Bases	2
2.1	Algebras	2
2.2	Motivation	3
2.3	Preliminary materials	4
3	Gröbner bases and Diamond lemma	6
3.1	Gröbner basis	6
3.2	Diamond lemma	7
4	Non-commutative Gröbner bases	11
5	Terminology for Gröbner bases	12
6	Computation of Gröbner bases	13
6.1	Buchberger's algorithm	13
6.2	In case of a commutative polynomial rings	13
6.3	In case of non-commutative polynomial rings	14

*Author is grateful to School of Mathematics, Trinity College Dublin for providing financial support to complete his masters research work there and Prof Vladimir Dotsenko for advising the thesis.

7	Hilbert series and it's computations	17
7.1	Graded algebra	17
7.2	Hilbert Series	17
7.3	Hilbert series for free product	20
7.4	Calculating Hilbert series through chains	21
8	Conclusion and Further work	23
9	References	23

1 Introduction

Suppose we have a polynomial ring (either commutative or non-commutative) in either one variable or multivariables. Also we are given an ideal I of that. Let f be a polynomial belonging to the ring. Now the question is whether it belongs to I or not? When we have a single variable polynomial ring, we can use our known division algorithm to say whether f belongs to I or not. But in case of a multivariable polynomial ring the computation is very complex as we can not apply our division algorithm. Then the concept of Gröbner bases easily solve this complexity.

Next we are aware of the concepts of Hilbert series for a graded spaces/algebras. We will use the concept of Gröbner bases to compute Hilbert series of some algebras through chains. This will lead us to find an exact sequence which can primarily satisfy our need but it can not tell us about the initial algebra. In the further work section we will mention about Anick's resolution which will fulfill the lack discussed in the previous section.

So let us begin with the concept of Gröbner bases:

2 Background for Gröbner Bases

2.1 Algebras

Definition 2.1.1. An **algebra** is a vector space V (over a field \mathbb{K}) equipped with a multiplication $V \otimes V \rightarrow V$ with the following properties:

- $(x + y)z = xz + yz$ for $x, y, z \in V$
- $x(y + z) = xy + xz$ for $x, y, z \in V$
- $(ab)(xy) = (ax)(by)$ where $x, y \in V$ and $a, b \in \mathbb{K}$.

Example 2.1.1. Algebra of polynomials $\mathbb{K}[x_1, x_2, \dots, x_n]$.

Definition 2.1.2. An algebra is **associative** if for the multiplication $\mu : V \otimes V \rightarrow V$ we have the equality

$$\mu(\mu \otimes id) = \mu(id \otimes \mu). \quad (1)$$

That associative algebra is called **commutative** if for any $v_1, v_2 \in V$ we have

$$\mu(v_1, v_2) = \mu(v_2, v_1). \quad (2)$$

It is **non-commutative** if the above equality fails for at least one pair of $v_1, v_2 \in V$.

Example 2.1.2. Algebra of commutative polynomials with either single or multivariables over a field \mathbb{K} is an example of commutative associative algebra. We usually denote it by $\mathbb{K}(x_1, x_2, \dots, x_n)$. However algebra of non-commutative polynomials are examples of non-commutative associative algebra and we usually denote it by $\mathbb{K}\langle x_1, x_2, \dots, x_n \rangle$.

2.2 Motivation

Suppose we have a polynomial ring (either commutative or non-commutative) in one variable, say $\mathbb{K}[x]$ where \mathbb{K} is the ground field. Suppose we have an ideal I of that ring $\mathbb{K}[x]$. Our job is to study the structure of $\mathbb{K}[x]/I$ in a constructive way. Later we will prove that the monomials not divisible by leading terms of the ideal I form a basis of $\mathbb{K}[x_1, x_2, \dots, x_n]/I$. We will use such facts to get to know that given a polynomial $f \in \mathbb{K}[x]$, does it belong to the ideal I or not? Now for single variable case it's easy as single variable polynomial ring $\mathbb{K}[x]$ is a Euclidean domain so we can perform Euclidean algorithm to know whether f belongs to I or not. But what for the case of multivariable polynomial ring $\mathbb{K}[x_1, x_2, \dots, x_n]$. Suppose we have the same question: we have an ideal $I \subset \mathbb{K}[x_1, x_2, \dots, x_n]$ and we are given a polynomial $f \in \mathbb{K}[x_1, x_2, \dots, x_n]$ and are asked whether f belongs to I or not. Now here the case is difficult as multivariable polynomial ring $\mathbb{K}[x_1, x_2, \dots, x_n]$ is neither a Euclidean domain nor a principal ideal domain.

Lemma 2.2.1. *The polynomial ring $\mathbb{K}[x_1, x_2, \dots, x_n]$ is not a principal ideal domain for $n > 1$.*

Proof. Take an ideal generated by $\{X_1, X_2\}$. If f generates this ideal, then f divides both X_1 and X_2 , so f is a constant term. So our ideal must be the entire ring. But 1 is in the ring, but not in the ideal. Contradiction. \square

To solve this problem we have the concept of Gröbner basis which is a type of basis defined carefully which tells that if we replace our generators f_i of the ideal I with a Gröbner basis g_j of the same ideal then we have the property that the remainder of f on division by the polynomials g_j is 0 if and only if f is in the ideal.

So we understand that to study the structure of $\mathbb{K}[x_1, x_2, \dots, x_n]/I$ in a constructive way we require the concept of Gröbner bases. The original definition was given in Bruno Buchberger's PhD thesis in 1965 [1]. Before moving to the definition of Gröbner bases we require some preliminary materials:

2.3 Preliminary materials

Theorem 2.3.1 (Hilbert basis theorem). *$I \subset \mathbb{K}[x_1, x_2, \dots, x_n]$ is always finitely generated, so there exist $f_1, f_2, \dots, f_m \in \mathbb{K}[x_1, x_2, \dots, x_n]$ such that $I = \langle (f_1, f_2, \dots, f_m) \rangle$.*

Definition 2.3.1. An **admissible ordering** " $<$ " of monomials is a total ordering of all monomials in $\mathbb{K}[x_1, x_2, \dots, x_n]$ such that

- it is a well ordering i.e. there is no infinite decreasing sequences.
- $m_1 < m_2 \Rightarrow m_1 m_3 < m_2 m_3$ for any monomial m_3 , where $m_1, m_2 \in \mathbb{K}[x_1, x_2, \dots, x_n]$.

Lemma 2.3.1. *There is only one admissible ordering of monomials in $\mathbb{K}[x]$ i.e.*

$$x^k < x^l \text{ if and only if } k < l$$

Proof. Proof of this is easy. We will take an ordering like this,

$$1 < x \text{ implies } x < x^2 \text{ implies } x^2 < x^3 \text{ implies } \dots$$

so we get an well ordering, so this is the admissible ordering. Now suppose we take $x < 1$ implies $x^2 < x$ implies $x^3 < x^2$ implies \dots , then this implies an infinite decreasing sequence, hence contradiction. \square

Remark 2.3.1. For $n \geq 2$, there are infinitely many admissible orderings.

Example 2.3.1. **LEX**(lexicographic ordering), it can be explained in this way,

$$x_1^{i_1} x_2^{i_2} x_3^{i_3} \dots x_n^{i_n} < x_1^{j_1} x_2^{j_2} x_3^{j_3} \dots x_n^{j_n}$$

if

$$\begin{aligned}
& i_1 < j_1 \text{ or} \\
& i_1 = j_1, i_2 < j_2 \text{ or} \\
& i_1 = j_1, i_2 = j_2, i_3 < j_3 \text{ or} \\
& \vdots
\end{aligned}$$

Example 2.3.2. DEGLEX(degree-lexicographic ordering), a little difference with **LEX** is that here first we consider the degree then the **LEX** ordering. It can be explained as follows,

$$x_1^{i_1} x_2^{i_2} x_3^{i_3} \dots x_n^{i_n} < x_1^{j_1} x_2^{j_2} x_3^{j_3} \dots x_n^{j_n}$$

if

$$\begin{aligned}
& i_1 + i_2 + i_3 + \dots + i_n < j_1 + j_2 + j_3 + \dots + j_n \text{ or} \\
& i_1 + i_2 + i_3 + \dots + i_n = j_1 + j_2 + j_3 + \dots + j_n \text{ and} \\
& x_1^{i_1} x_2^{i_2} x_3^{i_3} \dots x_n^{i_n} <_{\mathbf{LEX}} x_1^{j_1} x_2^{j_2} x_3^{j_3} \dots x_n^{j_n}.
\end{aligned}$$

Let us fix an admissible ordering. Let $I \subset \mathbb{K}[x_1, x_2, \dots, x_n]$ be an ideal. From this I we can find $\text{LT}(I)$ (leading terms) or we can say $\text{LT}(I)$ = space of linear combinations of monomials m over \mathbb{K} which are leading terms of elements of I . We say $m \in \text{LT}(I)$ if $\exists f \in I$ such that $f = cm + \sum c_i m_i$, where m_i 's are monomials with $m_i < m$ and $c_i \in \mathbb{K}$ and $c \neq 0$. However by $\text{LT}(f)$ for $f \in I$ we will mean the leading term of the polynomial according to our fixed admissible ordering. For an example we fix an order $x > y$, let our f be $x^2 + y^2$. Then $\text{LT}(f)$ is x^2 . Next by $\text{LC}(f)$ we mean the co-efficient of leading term of f . We denote leading co-efficient by LC .

Lemma 2.3.2. $\text{LT}(I)$ is itself an ideal in $\mathbb{K}[x_1, x_2, \dots, x_n]$.

Proof. It is very easy to show. Let we take our previous f i.e. $f = cm + \sum c_i m_i$, we form $m' = m''m$, multiplying m'' with the equation of f we get $f m'' = cm''m + \sum c_i m''m_i$, as I is an ideal so $f m'' \in I$ implies $m' \in \text{LT}(I)$. \square

Lemma 2.3.3. Cosets of monomials $m \notin \text{LT}(I)$ form a basis in $R = \mathbb{K}[x_1, x_2, \dots, x_n]/I$.

Proof. Let us first prove the linear independence.

Let $m_1, m_2, \dots, m_l \notin \text{LT}(I)$, without loss of generality assume $m_1 < m_2 < \dots < m_l$ (where $<$ is our fixed admissible ordering), then we have $c_1 m_1 + c_2 m_2 + \dots + c_l m_l = 0$ in R , where c_i 's $\in \mathbb{K}$. Let $f = c_1 m_1 + c_2 m_2 + \dots + c_l m_l$.

$\cdots + c_l m_l \in I$. Then $\text{LT}(f) \in \text{LT}(I)$, a contradiction unless $f = 0$ implies $c_1 = c_2 = \cdots = c_l = 0$.

Next job is to show the spanning set property i.e. we need to show that if $m \in \text{LT}(I)$, then m is a linear combination in R of cosets of monomials not present in $\text{LT}(I)$. We will prove this with the help of contradiction. Let's take the smallest $m \in \text{LT}(I)$ for which such a combination doesn't exist. Now by definition, $\exists f \in I$, such that $0 = f = cm + \sum c_i m_i$, with $m_i < m$, and each of m_i 's is not in $\text{LT}(I)$. Then we have $m = -\sum \frac{c_i}{c} m_i$ which can be represented as a combination of cosets of elements outside $\text{LT}(I)$. Contradiction. \square

3 Gröbner bases and Diamond lemma

3.1 Gröbner basis

Definition 3.1.1. $G \subset I$ is called a **Gröbner basis** of I if $\{\text{LT}(g) \mid g \in G\}$ generate the ideal $\text{LT}(I)$ i.e. for each $f \in I$, $\text{LT}(f)$ is divisible by $\text{LT}(g)$ for some $g \in G$.

Lemma 3.1.1. $\langle G \rangle = I$.

Proof. We know that $\langle G \rangle \subset I$, suppose assume that $\langle G \rangle \neq I$. Let $f \in I \setminus \langle G \rangle$ with smallest possible leading term. Then $\text{LT}(f) = m \text{LT}(g)$ for some $g \in G$, $m \in I$. Let $F = f - \frac{\text{LC}(f)}{\text{LC}(g)} mg$, where LC is the leading coefficient of leading term, then we have $\text{LT}(F) < \text{LT}(f)$, it implies $F \in I \Rightarrow F \in \langle G \rangle$, then $f = F + \frac{\text{LC}(f)}{\text{LC}(g)} mg \in \langle G \rangle$, which is a contradiction. \square

Remark 3.1.1. We have already proved that monomials not divisible by $\text{LT}(G)$ form a basis of $\mathbb{K}[x_1, x_2, \dots, x_n]/I$.

We are now going to define *reduction* and *S-polynomial* for the commutative case, these two definitions play an important role for computation of Gröbner bases. For all these definitions we have $\mathbb{K}(x_1, x_2, \dots, x_n)$ as the commutative ring.

Definition 3.1.2. Suppose f_1, f_2 are two polynomials belong to our defined ring, such that there exists a monomial m with

$$\text{LT}(f_1) = m \text{LT}(f_2).$$

Then

$$R_{f_2}(f_1) = f_1 - \frac{\text{LC}(f_1)}{\text{LC}(f_2)} m f_2 \quad (3)$$

is called **reduction** of f_1 with respect to f_2 .

Definition 3.1.3. We have two polynomials f_1 and f_2 in the ring, suppose there exist monomials m_1, m_2 such that

$$m_1 \text{LT}(f_2) = m_2 \text{LT}(f_1) \text{ and } \deg(m_1) < \deg \text{LT}(f_1) \quad (4)$$

then

$$S(f_1, f_2) = \frac{1}{\text{LC}(f_1)} m_2 f_1 - \frac{1}{\text{LC}(f_2)} m_1 f_2 \quad (5)$$

is called **S-polynomial** with respect to a small common multiple (4).

Example 3.1.1. Before giving the example, we would like to point out that throughout this paper $a \cdot b = ab$ for any a, b belonging to either field, algebras etc. Sometime for our better understanding and to deal with some scenarios we use the multiplication symbol \cdot .

Let us give an example to show how reduction and S-polynomial work, suppose we have a commutative polynomial ring in 2 variable i.e. $\mathbb{K}(x, y)$. We will pick **DEGLEX** ordering. Now let $f_1 = x^3 - y^2$ and $f_2 = x^3 - x + 1$. Then one can see for both f_1 and f_2 , LT is x^3 . So $\text{LT}(f_1) = \text{LT}(f_2) = x^3$ implies $m = 1$ so that $x^3 = 1 \cdot x^3$, our reduction of f_1 w.r.t f_2 will be then $x^3 - y^2 - (x^3 - x + 1) = x - y^2 - 1$.

And while computing S-polynomial with respect to a small common multiple we have 3 choices,

$$\begin{aligned} 1 \cdot x^3 &= 1 \cdot x^3 \\ x \cdot x^3 &= x \cdot x^3 \\ x^2 \cdot x^3 &= x^2 \cdot x^3 \end{aligned}$$

hence for each cases we can compute the S-polynomial using our formula (3). For an example if we consider $x \cdot x^3 = x \cdot x^3$ then our S-polynomial will be $x^2(x^3 - y^2) - x^2(x^3 - x + 1) = x^3 - x^2y^2 - x^2$.

Remark 3.1.2. In the commutative case S-polynomials for different common multiples are easily related, but in a non-commutative case, they all carry important information. We will see this when we will compute the Gröbner basis for non-commutative case.

3.2 Diamond lemma

Lemma 3.2.1. *Diamond lemma:*

$G \subset I$ forms a Gröbner basis if and only if for each $g_1, g_2 \in G$

$R_{g_2}(g_1)$ (if defined) can be reduced to 0 modulo G .

And also for each $g_1, g_2 \in G$ and each small common multiple of $\text{LT}(g_1), \text{LT}(g_2)$; the corresponding S-polynomial can be reduced to 0 modulo G .

We will write another lemma which is equivalent to the *diamond lemma*. We will prove this lemma only as it's easy to prove:

Lemma 3.2.2. *Assume $\langle G \rangle = I$, then the following statements are equivalent:*

1. *G is a Gröbner basis of I .*
2. *All reductions and all S -polynomials of pair of elements of G can be reduced to 0 modulo G .*
3. *For every $f \in I$, f admits a representation*

$$f = h_1g_1 + h_2g_2 + \cdots + h_ng_n; g_i \in G$$

with

$$\text{LT}(f) = \max(\text{LT}(h_i g_i))$$

Definition 3.2.1. f can be reduced to 0 modulo G , if there exists $g_1, g_2, \dots, g_n \in G$ such that

$$R_{g_n}(\dots R_{g_2}(R_{g_1}(f)) \dots) = 0$$

Proof. We need to show that

$$1 \text{ implies } 2 \text{ implies } 3 \text{ implies } 1$$

Now 3 implies 1 is trivial from the definition of Gröbner bases. We will at first prove 1 implies 2.

Suppose G is a Gröbner basis,

then every $f \in I$ can be reduced to 0 modulo G ,

($f \in I \Rightarrow \text{LT}(f) = m \text{LT}(g)$ for some $g \in G$, then $R_g(f)$ has smaller leading term and we proceed with that and proceed further until get 0.

Similarly for $f \in I$ we have $m_1 \text{LT}(f) = m_2 \text{LT}(g)$ for some $g \in G$, with $\deg(m_1) < \deg \text{LT}(g)$, so we have $S(f, g)$ with smaller leading term and proceed like this until get 0.)

This is exactly what statement (2) says.

Next we will show 2 implies 3.

As $I = \langle G \rangle$, let's take $f \in I$,

$$f = h_1g_1 + h_2g_2 + \cdots + h_ng_n; \text{ with } \text{LT}(f) < \max(\text{LT}(h_i g_i)).$$

Our main objective is to show how to replace this combination by another one with smaller $\max(\text{LT}(h_i g_i))$, if still bigger than $\text{LT}(f)$, continue until it becomes $\text{LT}(f)$. Without loss of generality,

$$\text{LT}(h_1g_1) = \text{LT}(h_2g_2) = \cdots = \text{LT}(h_kg_k) = \max \text{LT}(h_i g_i)$$

and $\text{LT}(h_p g_p) < \max \text{LT}(h_i g_i)$ for $p > k$.

We will use induction on k to prove our desired result.
if $k = 1$, a contradiction as we can't cancel, so $k \geq 2$. Now

$$\text{LT}(h_1 g_1) = \text{LT}(h_1) \text{LT}(g_1)$$

$$\text{LT}(h_2 g_2) = \text{LT}(h_2) \text{LT}(g_2).$$

Without loss of generality assume these 3 conditions:

1. $\text{LT}(g_1)$ is divisible by $\text{LT}(g_2)$.
2. $\text{LT}(g_1), \text{LT}(g_2)$ have a small common multiple.
3. $\text{LT}(g_1), \text{LT}(g_2)$ have no common divisors.

Let us first deal with (1),

$$\text{LT}(g_1) = m \text{LT}(g_2)$$

$$\text{then } R_{g_2}(g_1) = g_1 - \frac{\text{LC}(g_1)}{\text{LC}(g_2)} m g_2$$

$$\text{now } h_1 g_1 + h_2 g_2 = h_1 \left(R_{g_2}(g_1) + \frac{\text{LC}(g_1)}{\text{LC}(g_2)} m g_2 \right) + h_2 g_2$$

$$= h_1 R_{g_2}(g_1) + \left(\frac{\text{LC}(g_1)}{\text{LC}(g_2)} m h_1 + h_2 \right) g_2$$

$$\text{with } \text{LT}(R_{g_2}(g_1)) < \text{LT}(g_1)$$

$$\text{so } h_1 R_{g_2}(g_1) = \sum_i \tilde{h}_i g_i h_1$$

$$\text{LT}(g_1) > \text{LT}(R_{g_2}(g_1)) = \max(\text{LT}(\tilde{h}_i g_i))$$

So (1) replace the combination by another one with smaller k . Lets move to case (2),

$$\text{LT}(h_1) \text{LT}(g_1) = \text{LT}(h_2) \text{LT}(g_2)$$

suppose that,

$$\text{LT}(g_1) = m_1 d$$

$$\text{LT}(g_2) = m_2 d$$

where m_1, m_2 have no common factors,

$$\text{LT}(h_1) m_1 d = \text{LT}(h_2) m_2 d$$

canceling d from both side we get,

$$\text{LT}(h_1) = e m_2$$

$$\text{LT}(h_2) = em_1, \quad \text{for some } e,$$

$$\begin{aligned} h_1g_1 + h_2g_2 &= \text{LC}(h_1) \text{LT}(h_1)g_1 + (h_1 - \text{LC}(h_1) \text{LT}(h_1))g_1 \\ &\quad + \text{LC}(h_2) \text{LT}(h_2)g_2 + (h_2 - \text{LC}(h_2) \text{LT}(h_2))g_2 \end{aligned}$$

as $(h_1 - \text{LC}(h_1) \text{LT}(h_1))g_1 + (h_2 - \text{LC}(h_2) \text{LT}(h_2))g_2$ have smaller leading term so we will not consider this in our account and proceed with the remaining terms, i.e. we deal with

$$\text{LC}(h_1) \text{LT}(h_1)g_1 + \text{LC}(h_2) \text{LT}(h_2)g_2. \quad (6)$$

We have

$$m_2 \text{LT}(g_1) = m_1 \text{LT}(g_2)$$

so the S-polynomial w.r.t small common multiple,

$$S = \frac{1}{\text{LC}(g_1)}m_2g_1 - \frac{1}{\text{LC}(g_2)}m_1g_2$$

Putting the values of $\text{LT}(h_1)$ and $\text{LT}(h_2)$ in eq (6) we get,

$$\begin{aligned} &\text{LC}(h_1)em_2g_1 + \text{LC}(h_2)em_1g_2 \\ &= \text{LC}(h_1) \left(\text{LC}(g_1)S + \frac{\text{LC}(g_1)}{\text{LC}(g_2)}m_1g_2 \right) e + \text{LC}(h_2)em_1g_2 \\ &= \text{LC}(h_1) \text{LC}(g_1)S + \left(\text{LC}(h_1) \frac{\text{LC}(g_1)}{\text{LC}(g_2)}m_1e + \text{LC}(h_2)m_1e \right) g_2 \end{aligned}$$

So we have again replaced the combination with a smaller k .

Finally we have case (3) in hand,

$$\text{LT}(h_1) \text{LT}(g_1) = \text{LT}(h_2) \text{LT}(g_2)$$

$$\Rightarrow \text{LT}(h_1) = \text{LT}(g_2)e$$

$$\text{and } \text{LT}(h_2) = \text{LT}(g_1)e, \quad \text{for some } e$$

Now

$$\begin{aligned} &h_1g_1 + h_2g_2 \\ &= \text{LC}(h_1) \text{LT}(h_1)g_1 + \text{LC}(h_2) \text{LT}(h_2)g_2 + \text{lower terms.} \end{aligned}$$

Then proceed with

$$\text{LC}(h_1) \text{LT}(h_1)g_1 + \text{LC}(h_2) \text{LT}(h_2)g_2$$

replacing the values of $\text{LT}(h_1)$ and $\text{LT}(h_2)$,

$$= \text{LC}(h_1) \text{LT}(g_2)eg_1 + \text{LC}(h_2) \text{LT}(g_1)eg_2. \quad (7)$$

We have

$$\text{LT}(g_2) = \frac{1}{\text{LC}(g_2)}(g_2 - \bar{g}_2),$$

replacing this in eq (7) we get

$$\frac{\text{LC}(h_1)}{\text{LC}(g_2)}(g_2 - \bar{g}_2)eg_1 + \text{LC}(h_2) \text{LT}(g_1)eg_2$$

which again makes either LT on k smaller.

This is how we proceed using induction and prove statement (3) from (2). \square

4 Non-commutative Gröbner bases

We consider the non-commutative polynomial ring $\mathbb{K}\langle x_1, x_2, \dots, x_n \rangle$.

Definition 4.0.2. We have two polynomials f, g belong to the above ring, with there exists monomials m_1, m_2 such that,

$$\text{LT}(f) = m_1 \text{LT}(g)m_2$$

then

$$R_g(f) = f - \frac{\text{LC}(f)}{\text{LC}(g)}m_1gm_2 \quad (8)$$

is called **reduction** of f with respect to g .

Definition 4.0.3. For f, g of the ring and for any small common multiple of $\text{LT}(f), \text{LT}(g)$; there exists two monomials m_1, m_2 with

$$\text{LT}(f)m_2 = m_1 \text{LT}(g) \text{ with } \deg m_1 < \deg \text{LT}(f)$$

then

$$S(f, g) = \frac{1}{\text{LC}(f)}f m_2 - \frac{1}{\text{LC}(g)}m_1 g \quad (9)$$

is called the **S-polynomial** with respect to small common multiples.

Remark 4.0.1. $I \subset \mathbb{K}\langle x_1, x_2, \dots, x_n \rangle$ is a two-sided ideal. Then $\text{LT}(I)$ which is linear span of $\text{LT}(f)$ with $f \in I$ is also a two-sided ideal.

Definition 4.0.4. $G \subset I$ is a **Gröbner basis** of I if for every $f \in I$, we have $\text{LT}(f) = m_1 \text{LT}(g)m_2$ for some $g \in G$.

Lemma 4.0.3 (Diamond lemma for non-commutative case). $G \in I$ forms a Gröbner basis of I if and only if for each $g_1, g_2 \in G$; $R_{g_2}(g_1)$ (if defined) can be reduced to 0 modulo G . Also for each $g_1, g_2 \in g$ and each small common multiple of $\text{LT}(g_1), \text{LT}(g_2)$; the corresponding S -polynomial can be reduced to 0 modulo G .

Proof. As the proof is similar like the commutative case so we will skip this. \square

5 Terminology for Gröbner bases

Before moving towards the computation of Gröbner bases for both commutative and non-commutative cases we will first give some terminology regarding Gröbner bases.

Definition 5.0.5. Normal monomial:

Given a Gröbner basis $G \subset I$, normal monomials with respect to G are those monomials which are not divisible by $\text{LT}(g)$, for $g \in G$.

We sometime call normal monomials as normal words.

Lemma 5.0.4. *Cosets of normal monomials form a basis of $\mathbb{K}[x_1, x_2, \dots, x_n]/I$.*

Proof. This is proved earlier in lemma 2.3.3 \square

Definition 5.0.6. Reduced Gröbner basis:

G , a Gröbner basis of I is reduced if for each $g \in G$,

- $\text{LC}(g) = 1$.
- $g - \text{LT}(g)$ is a linear combination of normal monomials.

Theorem 5.0.1. *Let us fix an admissible ordering. Then every I has a unique reduced Gröbner basis.*

Proof. Let us take some Gröbner basis $G \subset I$.

First condition of reduced Gröbner basis is easy to satisfy as we just divide each g by it's LC, i.e. $g \rightarrow g / \text{LC}(g)$.

The reduction and S -polynomial suggests that remaining terms of g is not divisible by the leading term of any terms in G which implies that $g - \text{LT}(g)$ is a linear combination of normal monomials. Now we will prove the uniqueness.

Let $\{f_1, f_2, \dots, f_s\}$ and $\{g_1, g_2, \dots, g_s\}$ be two reduced and ordered Gröbner bases so that $\text{LT}(f_i) = \text{LT}(g_i)$ for each i . Consider $f_i - g_i \in I$, if it's not 0, then its leading term must be a term that appeared either in f_i or in g_i . In either case, this contradicts the fact that the bases being reduced, so in fact we get our required $f_i = g_i$. \square

6 Computation of Gröbner bases

In this section we will show how to compute Gröbner basis for an ideal I of a polynomial ring $\mathbb{K}[x_1, x_2, \dots, x_n]$. We will show for both commutative and non-commutative polynomial rings. So let us begin with a computation for a commutative polynomial ring. But at first we will show the general algorithm to compute the Gröbner basis.

6.1 Buchberger's algorithm

We start with an ideal I generated by a set G . The Buchberger's algorithm[2], which is a simple consequence of lemma 3.1.2, is the following:

Step 1: If the leading term of any element u of G occurs inside the leading term of another element v of G , then we reduce v by subtracting off the required multiple of u . In general we will perform the reduction mentioned in either definition 3.1.2 or definition 4.0.5.

Step 2: For each pair of distinct elements of G (for both commutative and non-commutative cases) or even in non-commutative case for a same element we compute the S-polynomial and a remainder of it.

Step 3: If the remainder can be reduced further then we will follow step 1 or we will add that term in our set G . If all S-polynomials reduce to 0, then the algorithm ends and G is the Gröbner basis of I . If not then we will continue further with our 3 steps.

For commutative cases the algorithm ends in a finite number of stages. However for a non-commutative case there is no guarantee of the termination of the algorithm after a finite number of stages. In that case we start adding all elements which can't be reduced further in our set G and in most cases we have seen a combinatorial interpretation for our terms in G .

6.2 In case of a commutative polynomial rings

Example 6.2.1. We have previously defined what is meant by a commutative polynomial ring. Let us take $\mathbb{K}(x_1, x_2)$ as our commutative polynomial ring with two variables x_1, x_2 . Suppose there are two polynomials

$$h_1(x_1, x_2) = x_1^2 + x_2^2$$

$$h_2(x_1, x_2) = x_1^3 + x_2^3$$

belonging to our polynomial ring $\mathbb{K}(x_1, x_2)$. We will compute the Gröbner basis for $I = (h_1, h_2) \subset \mathbb{K}(x_1, x_2)$.

Let us fix an admissible ordering. Usually we take **DEGLEX** ordering. So

here we consider $x_1 > x_2$. So we get $\text{LT}(h_1) = x_1^2$ and $\text{LT}(h_2) = x_1^3$. So initially our set is $G = \{h_1, h_2\}$. But we see that h_2 can be reduced further. So we have $x_1^3 = x_1 \cdot x_1^2$,

$$\begin{aligned} R_{h_1}(h_2) &= (x_1^3 + x_2^3) - x_1(x_1^2 + x_2^2) \\ &= x_2^3 - x_1x_2^2. \end{aligned}$$

So we have obtained a new term $x_2^3 - x_1x_2^2$ which cannot be reduced further, we add this to our set G which is now $\{h_1, R_{h_1}(h_2)\}$. We call $R_{h_1}(h_2)$ as h_3 . We see that the leading term of h_3 is $x_1x_2^2$. We have also found that $x_1 \cdot x_1x_2^2 = x_1^2 \cdot x_2^2$. So we will compute the S-polynomial between h_1, h_3 .

$$\begin{aligned} S(h_1, h_3) &= -x_1(x_2^3 - x_1x_2^2) - (x_1^2 + x_2^2)x_2^2 \\ &= -x_1x_2^3 - x_2^4. \end{aligned}$$

The term $-x_1x_2^3 - x_2^4$ has $x_1x_2^3$ as the leading term which can be reduced further through $\text{LT}(h_3)$. We get $x_1x_2^3 = (x_1x_2^2) \cdot x_2$. hence the reduction yields

$$\begin{aligned} -x_1x_2^3 - x_2^4 - (x_2^3 - x_1x_2^2)x_2 \\ = -2x_2^4 \end{aligned}$$

which cannot be reduced further and also one cannot compute more S-polynomial. Hence we add $-2x_2^4$ in our set G and the final set G is our Gröbner basis for I , the set is precisely as follows

$$\{x_1^2 + x_2^2, x_2^3 - x_1x_2^2, -2x_2^4\}.$$

Remark 6.2.1. The reduced Gröbner basis of I of our previous example is given by $\{x_1^2 + x_2^2, x_1x_2^2 - x_2^3, x_2^4\}$. It is not very difficult to obtain this reduced Gröbner basis from our computed Gröbner basis. If we recall the definition of reduced Gröbner basis we will see that all leading co-efficients of the reduced basis should be 1. So we just divide terms $-2x_2^4, x_2^3 - x_1x_2^2$ of $\{x_1^2 + x_2^2, x_2^3 - x_1x_2^2, -2x_2^4\}$ by -2 and -1 respectively to obtain $\{x_1^2 + x_2^2, x_1x_2^2 - x_2^3, x_2^4\}$. Indeed x_2^2 and x_2^3 are normal monomials. So we have obtained the reduced Gröbner basis of I .

6.3 In case of non-commutative polynomial rings

Example 6.3.1. Let us consider $\mathbb{K}\langle x, y \rangle$ as a non-commutative polynomial ring. We are going to compute Gröbner basis for $I = (x^2 - xy)$. So we begin with our set G as $\{x^2 - xy\}$ whose leading term is x^2 (we consider the

DEGLEX for this case i.e. here $x > y$). We need to compute S-polynomial between polynomial $f_1 = x^2 - xy$ and $f_2 = x$. We have $x^2 \cdot x = x \cdot x^2$. Then

$$\begin{aligned} S(f_1, f_2) &= (x^2 - xy)x - x(x^2 - xy) \\ &= xxy - xyx. \end{aligned}$$

We see that $xyx - xyx$ whose leading term is xyx can be reduced further. So we have $xyx = x^2 \cdot y$. So the reduction is

$$\begin{aligned} &(xxy - xyx) - (x^2 - xy)y \\ &= xxy - xyx - x^2y + xyy \\ &= xyy - xyx \end{aligned}$$

which cannot be reduced further. so we include $xyy - xyx$ in our set G which is now $\{x^2 - xy, xyy - xyx\}$. We see that $x^2 \cdot yx = x \cdot xyx$, hence we compute S-polynomial between those elements of our set G and we get

$$\begin{aligned} &(x^2 - xy)yx + x(xyy - xyx) \\ &= x^2yx - xyyx + xxyy - xxyx \\ &= xxyy - xyyx \end{aligned}$$

this element with leading term xyy can be reduced further and we get $xyy = x^2 \cdot yy$. So the reduction gives

$$\begin{aligned} &(xxyy - xyyx) - (x^2 - xy)yy \\ &= xxyy - xyyx - x^2yy + xyyy \\ &= xyyy - xyyx \end{aligned}$$

which cannot be reduced further and we add this term in our existing set G and obtain $\{x^2 - xy, xyy - xyx, xyyy - xyx\}$.

Now we claim that the Gröbner basis for $I = (x^2 - xy)$ is given by

$$\{x^2 - xy\} \cup \bigcup_{i=2}^{\infty} \{xy^i - xy^{i-1}x\}.$$

This is indeed very easy to prove. We will prove it by method of induction. We have already shown for $i = 2, 3$. Suppose upto $i = k$ steps the Gröbner basis of I is

$$\{x^2 - xy\} \cup \bigcup_{i=2}^k \{xy^i - xy^{i-1}x\}.$$

But none of $\{xy^i - xy^{i-1}x\}$ for $2 \leq i \leq k$ have S-polynomial between them, so $\text{LT}(xy^k - xy^{k-1}x) = xy^{k-1}x$ and we have $x^2 \cdot y^{k-1}x = x \cdot xy^{k-1}x$ which leads us to compute the s-polynomial between $x^2 - xy$ and $xy^k - xy^{k-1}x$ and we get

$$\begin{aligned} & (x^2 - xy)y^{k-1}x + x(xy^k - xy^{k-1}x) \\ &= x^2y^{k-1}x - xy^kx + x^2y^k - x^2y^{k-1}x \\ &= x^2y^k - xy^kx \end{aligned}$$

which has the leading term x^2y^k which can be reduced further. We get $x^2y^k = x^2 \cdot y^k$. Hence the reduction is

$$\begin{aligned} & (x^2y^k - xy^kx) - (x^2 - xy)y^k \\ &= xy^{k+1} - xy^kx \end{aligned}$$

which cannot be reduced further and so we add the term $xy^{k+1} - xy^kx$ in our existing set G .

Hence the proof and we have obtain our said Gröbner basis.

Example 6.3.2. Let us give another example to compute Gröbner basis for a non-commutative polynomial ring. Consider $\mathbb{K}\langle x, y, z \rangle$ as our non-commutative polynomial ring. We are going to compute Gröbner basis for $I = (x^2, xy - zx)$. We will consider **DEGLEX** ordering, so we consider $x > y > z$. The leading terms of x^2 and $xy - zx$ are x^2 and xy respectively and both of them cannot be reduced further. So our initial set G is $\{x^2, xy - zx\}$. However we can compute S-polynomial between them based on $x^2 \cdot y = x \cdot xy$ and obtain

$$\begin{aligned} & x^2y - x(xy - zx) \\ &= xzx \end{aligned}$$

which cannot be reduced further and so include it in our set G . So now our set G is $\{x^2, xy - zx, xzx\}$. We can compute S-polynomial between $xy - zx$ and xzx . We have $xzx \cdot y = xz \cdot xy$ and so our S-polynomial is

$$\begin{aligned} & (xzx)y - xz(xy - zx) \\ &= xzzx \end{aligned}$$

which cannot be reduced further so we add it to G and get $\{x^2, xy - zx, xzx, xzzx\}$. This is how we proceed and claim that Gröbner basis for I is given by

$$\{x^2, xy - zx\} \cup \bigcup_{i=1}^{\infty} \{xz^i x\}.$$

We can prove this using the similar argument we have used in the previous example by method of induction.

7 Hilbert series and it's computations

7.1 Graded algebra

Definition 7.1.1. An algebra A is **graded** if:

- $A = \bigoplus_{i=0}^{\infty} A_i$
- $A_i A_j \subseteq A_{i+j}$.

Example 7.1.1. The polynomial algebra is graded by degree.

7.2 Hilbert Series

Our main goal is to find tools to investigate properties of algebras. One of the main properties we are interested in is the size of an algebra. Most algebras we will be considering are infinite dimensional, so the question needs to be better defined. In the graded case at least, this is simple - we can ask the dimension of each graded component. This gives a sequence of numbers, which describes the size of the entire algebra. When we have a sequence of numbers, we can talk about the generating function. This is called *Hilbert series* for our graded algebra.

Definition 7.2.1. Let $A = \bigoplus_{n=0}^{\infty} A_n$ be a graded algebra. Then the formal series

$$H_A = \sum_{n=0}^{\infty} \dim(A_n) t^n$$

is called the **Hilbert series** of the algebra A .

Example 7.2.1. Let us give an example - how to find the Hilbert series of the free associative algebra $A = \mathbb{K}\langle x, y, z \rangle$.

One can easily see that this algebra is graded - the graded components are homogeneous subspaces of each degree. So the subspace of degree 0 has dimension 1. The subspace of degree 1 is generated by x, y, z . So that has dimension 3. The subspace of degree 2 is generated by $x^2, xy, xz, yx, y^2, yz, zx, zy, z^2$, which is of dimension 9.

In general, the subspace of degree n has dimension 3^n (as there are 3 independent choices for each of the n positions). So

$$H_A = \sum_{n=0}^{\infty} 3^n t^n = \frac{1}{1-3t}$$

Theorem 7.2.1. *If we have two graded algebras U and V , then we grade the algebra $U \oplus V$ with components $U_n \oplus V_n$ (except when $n = 0$, in which case $(U \oplus V)_n = K$). Similarly we can define the graded components of $U \otimes V$ as $\sum_{i=0}^n U_i \otimes V_{n-i}$. Then*

$$H_{U \oplus V} = H_U + H_V$$

and

$$H_{U \otimes V} = H_U H_V$$

Proof. For the first equality, we simply note that:

$$\dim(U \oplus V)_n = \dim U_n + \dim V_n.$$

For the second,

$$\dim(U \otimes V)_n = \sum_{i=0}^n \dim U_i \dim V_{n-i}$$

this exactly matches the co-efficient of t^n in $H_U H_V$. \square

Corollary 7.2.1. *We call a subspace V homogeneous if $V = \bigoplus A_n \cap V$. If U, V are homogeneous subspaces of some algebra, then $H_{U+V} \leq H_U + H_V$ and $H_{UV} \leq H_U H_V$ (where the inequality is co-efficient wise, and the sum and product are set sum and multiplications).*

Proof. This directly follows from theorem 7.2.1. We have equality if every element of H_{U+V} can be written uniquely as $u + v$. \square

Lemma 7.2.1. *If A is an algebra with set of normal words N , then $H_A = H_N$.*

Proof. A is the free associative algebra, mod some ideal I . The free associative algebra itself decomposes into $N \oplus I$, so it's Hilbert series can be written as $H_N + H_I$. Modding out by I turns the free algebra into our algebra A , and kills the H_I term. So $H_A = H_N$ as required. \square

Example 7.2.2. (Hilbert series of polynomial algebra):

Let us give another example - how to find the Hilbert series of the polynomial algebra $A = \mathbb{K}[x, y]$.

Again we can take grading by degree. So the subspace of degree 0 has dimension 1. The subspace of degree 1 is generated by x, y , so it has dimension 2. The subspace of degree 2 is generated by x^2, xy, y^2 , which has dimension 3.

In general, the subspace of degree n has dimension $n + 1$ (as the word is

determined by the position where the x 's stop and the y 's begin; there are $n + 1$ such places). So

$$H_A = \sum_{n=0}^{\infty} (n+1)t^n$$

we note that

$$\frac{1}{1-t} = \sum_{n=0}^{\infty} t^n.$$

Taking derivatives on both sides give:

$$\frac{1}{(1-t)^2} = \sum_{n=0}^{\infty} (n+1)t^n$$

So

$$H_A = \frac{1}{(1-t)^2}$$

Theorem 7.2.2. *The Hilbert series of the polynomial algebra $\mathbb{K}[X]$ is computed by the formula*

$$H_{\mathbb{K}[X]} = \prod_{x \in X} (1 - t^{|x|})^{-1}.$$

The Hilbert series of the exterior algebra $\bigwedge \mathbb{K}[X]$ is calculated by the formula

$$H_{\bigwedge \mathbb{K}[X]} = \prod_{x \in X} (1 + t^{|x|}).$$

In particular, in case of natural graduation and a finite set of generators d , we have:

$$H_{\mathbb{K}[X]}^{-1} = (1-t)^d; \quad H_{\bigwedge \mathbb{K}[X]} = (1+t)^d$$

Proof. In the case of one generator, the Hilbert series in the power of $n = |x|$ is computed straightforwardly: it is equal to $1 + t^n + t^{2n} + \dots = (1 - t^n)^{-1}$ in case of polynomial ring and $1 + t^n$ in the case of exterior algebra. The case of finite number of generators reduces to this one, with the help of theorem 7.2.1. Finally, in case of infinite number of generators, the degree of generators must increase, for if not, we do not get finite-dimensionality. Consequently, for every n , the segment of the Hilbert series up to the exponent n depends only on finite number of generators with the degree not exceeding n , thus everything reduces to the finite case. \square

Remark 7.2.1. If we apply the formula of Hilbert series for polynomial algebra of theorem 7.2.2 to our previous computed example 7.2.2 we will get the exact result.

7.3 Hilbert series for free product

Definition 7.3.1. We define the **free product** of two algebra A, B as the disjoint union of their generators, with both sets of relations. We usually denote it by $A * B$.

Example 7.3.1. The free product of the algebra $A = \langle x \mid x^3 + 2x^2 \rangle$ and the algebra $B = \langle x, y \mid 2x^2 = y^2 \rangle$ is given by the algebra $A * B = \langle x, y, z \mid x^3 + 2x^2, 2y^2 = z^2 \rangle$.

Theorem 7.3.1 (Hilbert series of free product). *If A, B are graded algebras, then*

$$(H_{A*B})^{-1} = H_A^{-1} + H_B^{-1} - 1.$$

Proof. Any word/monomial in $A * B$ is either begins with a (non-scalar) element of A , or an element of B (excluding terms that belong to the underlying field). This follows from the fact that, because the two sets of generators have no overlap, the Gröbner basis of $A * B$ will be the union of the Gröbner basis of A and the Gröbner basis of B . So take any monomial in $A * B$. It begins with a generator either from A or B . Without loss of generality say its from A . Then take the longest prefix of this word that consists of generators from A . This must be a word in A , otherwise it would contain a leading term of the Gröbner basis for A , and hence a leading term in the Gröbner basis for $A * B$.

So we know that words in $A * B$ start with a word from either A or B . That suggests the following decomposition:

$$H_{A*B} = H_{V_1} + H_{V_2} + 1$$

where V_1 are the elements that begin with a non-scalar element of A , and V_2 are the elements that begin with a non-scalar element of B . So we have

$$H_{V_1} = (H_A - 1)(H_{V_2} + 1)$$

$$H_{V_2} = (H_B - 1)(H_{V_1} + 1).$$

The above imply that

$$H_{V_1} = \frac{H_A H_B - H_B}{H_A + H_B - H_A H_B}$$

$$H_{V_2} = \frac{H_A H_B - H_A}{H_A + H_B - H_A H_B}$$

So

$$H_{A*B} = \frac{H_A H_B - H_B}{H_A + H_B - H_A H_B} + \frac{H_A H_B - H_A}{H_A + H_B - H_A H_B} + 1$$

$$\begin{aligned}
&= \frac{2H_A H_B - H_A - H_B - H_A H_B + H_A + H_B}{H_A + H_B - H_A H_B} \\
&= \frac{H_A H_B}{H_A + H_B - H_A H_B}.
\end{aligned}$$

Hence

$$(H_{A*B})^{-1} = H_A^{-1} + H_B^{-1} - 1.$$

□

7.4 Calculating Hilbert series through chains

Let $A = \mathbb{K}\langle X \mid R \rangle$ be an algebra where X is the set of generators and R is the set of relations. Let the set of normal words be N , and say we have a reduced Gröbner basis G . Let F be the set of leading terms of G - we call the elements of F *obstructions*. A word is normal with respect to G if and only if it does not contain any of the elements of F as a subword. Thus a word s is normal with respect to G if and only if it's normal with respect to F . Therefore the algebra $\hat{A} = \mathbb{K}\langle X \mid F \rangle$ has the same normal words as A . And so $H_A = H_{\hat{A}}$. The advantage of dealing with F instead of G is that F consists of monomials only, which makes it much easier to deal with.

Definition 7.4.1 (Chains). A (-1) -chain is the empty word and is its own tail. The 0-chains are the elements of the generating set X , and are also their own tails. We will define chain inductively: a n -chain is a word f of the form gt , with some conditions on g and t . Firstly, g must be a $(n-1)$ -chain and t is a normal word. Secondly, if r is the tail of g then $\deg_F rt = 1$; that is, the word rt contains exactly one element of F as a subword. This subword must occur at the end of rt . The tail of gt is defined to be t . We denote the space spanned by n -chains by C_n .

Example 7.4.1. Let $F = \{x^3\}$. The unique 1-chain is $x^3 = x \cdot x^2$ and its tail is x^2 . Then the unique 2-chain is $\overline{xxx} = x^3 \cdot x$. The word $x^3 \cdot x^2$ is not a 2-chain, since $\deg_F x^2 x^2 = 2$. The unique 3-chain is the word $x^6 = x^4 x^2$. The word $x^5 = x^4 x$ is not a 3-chain because $\deg_F x \cdot x = 0$, regardless of the fact that it can be represented $(xxxxx)$ as a link of three obstructions \overline{xxx} (the fact is that the first one intersects with the last one).

In general the n -chain is given by $x^{n+1} \cdot x$ if n is even and $x^{n+1} \cdot x^2$ if n is odd. We see that in this case for every n there exists only one n -chain.

Theorem 7.4.1. *Let*

$$\dots \xrightarrow{d_{n+1}} A_n \xrightarrow{d_n} A_{n-1} \xrightarrow{d_{n-1}} \dots \xrightarrow{d_{k+1}} A_k \xrightarrow{d_k} K \longrightarrow 0$$

be an exact sequence of graded spaces (i.e $\ker d_i = \text{Im } d_{i+1}$). Then

$$\sum_{i=k}^{\infty} (-1)^i H_{A_i} = (-1)^k$$

if the sum is well defined.

Proof. We know that if $f : V \rightarrow W$ is any linear transformation such that $f(V_n) \subset f(W_n)$, then $H_V = H_{\ker f} + H_{\text{Im } f}$. So

$$H_{A_i} = H_{\ker d_i} + H_{\text{Im } d_i} = H_{\text{Im } d_{i+1}} + H_{\text{Im } d_i},$$

where the second equality comes from exactness. Thus taking the alternating sum of these equalities, we get our required result. \square

Theorem 7.4.2 (Hilbert series from chains). *Let A be an algebra and C_n be the linear span of n -chains. We point out that*

$$H_{C_{-1}} = H_K = 1; \quad H_{C_0} = H_X; \quad H_{C_1} = H_F.$$

Then

$$H_A = (H_{C_{-1}} - H_{C_0} + H_{C_1} - H_{C_2} + \dots)^{-1}.$$

Proof. Let $\hat{A} = \mathbb{K}\langle X \mid F \rangle$ where F is our set of obstructions. Let $d_n : C_n \otimes \hat{A} \rightarrow C_{n-1} \otimes \hat{A}$ be defined by $d_n(gt \otimes a) = g \otimes ta$. Then $d_n(d_{n+1}(gt \otimes a)) = d_n(g \otimes ta) = g' \otimes t'ta$, where $g \in C_n$, $g' \in C_{n-1}$. By the definition of n -chains it follows that there must be an obstruction in $t'ta$, so this is 0.

Also d_n is a surjection, as for every $g \otimes a \in C_{n-1} \otimes \hat{A}$, we can decompose a as $a_1 a_2$ such that $ga_1 \otimes a_2 \in C_n \otimes \hat{A}$. So we have an exact sequence:

$$\dots \xrightarrow{d_{n+1}} C_n \otimes \hat{A} \xrightarrow{d_n} C_{n-1} \otimes \hat{A} \xrightarrow{d_{n-1}} \dots \xrightarrow{d_0} C_{-1} \otimes \hat{A} \longrightarrow K \longrightarrow 0$$

So by theorem 7.4.1

$$\sum_{i=-1}^{\infty} (-1)^i H_{C_i \otimes \hat{A}} = -1.$$

Now $H_{C_i \otimes \hat{A}} = H_{C_i} H_{\hat{A}} = H_{C_i} H_A$. Hence

$$H_A = (H_{C_{-1}} - H_{C_0} + H_{C_1} - H_{C_2} + \dots)^{-1}.$$

\square

Example 7.4.2. Let $A = \mathbb{K}\langle x, y \mid x^2 + y^2 \rangle$. The obstructions of A are x^2 and xy^2 (the Gröbner basis of A is $\{x^2 + y^2, xy^2 - y^2x\}$). We have found that the n -chains are given by $x^n y^2$ and x^{n+1} , for $n > 0$. So we have,

$$H_A^{-1} = (1 - 2t + (t^2 + t^3) - (t^3 + t^4) + \dots) = 1 - 2t + t^2.$$

Hence

$$H_A = \frac{1}{1 - 2t + t^2}.$$

8 Conclusion and Further work

In the proof of theorem 7.4.2, we have constructed a resolution for the normal words of our algebra. This allows us to find the Hilbert series for our normal words and hence for our original algebra. However this resolution only depends on normal words, so the rest of the structure of our algebra is lost. This is okay if we are only interested in the size of algebra. If we want more properties of the algebra then this leads to a construction of a resolution of the algebra itself. Along with this fact, that sequence and isomorphism of spaces with graduations $C_n \otimes \hat{A}$ and $C_n \otimes A$ leads us to think about the existence of a corresponding free resolution which was constructed by Anick. We refer [3] as a good reference to study Anick's resolution to the interested readers.

9 References

1. Bruno Buchberger, An Algorithm for Finding the Basis Elements of the Residue Class Ring of a Zero Dimensional Polynomial Ideal, Ph.D. Dissertation, 1965. *Journal of Symbolic Computation*, **41**, 2006 (Translation).
2. Viviana Ene - Jürgen Herzog, *Gröbner Bases in Commutative Algebra*, Graduate Studies in Mathematics, Volume 130, AMS.
3. V.A.Ulfarovskij, *Combinatorial and Asymptotic Methods in Algebra*. pp.- 42-58. Algebra VI, Springer, 1995.

SCHOOL OF MATHEMATICS, TRINITY COLLEGE DUBLIN, DUBLIN 2
E-mail address— `roychows@maths.tcd.ie`